UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/977,192	10/16/2001	Stefan Andersson	0119-082	3198

42015 7590 03/18/2009
POTOMAC PATENT GROUP PLLC
P. O. BOX 270
FREDERICKSBURG, VA 22404

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
03/18/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

tammy@ppglaw.com

Office Action Summary	Application No.	Applicant(s)	
	09/977,192	ANDERSSON, STEFAN	
	Examiner	Art Unit	
	JEFFERY WILLIAMS	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/21/08*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 – 19, 24 – 30, 32 – 52* is/are pending in the application.

4a) Of the above claim(s) *51 and 52* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 – 19, 24 – 30, 32 – 50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 January 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1 – 19, 24 – 30, 32 – 52 are pending.

Claims 51 and 52 are withdrawn from consideration.

This action is in response to the communication filed on 11/21/08.

All objections and rejections not set forth below have been withdrawn.

Election/Restrictions

Applicant's election of claims 1-19,24-30, and 32-50 in the reply filed on 11/21/08 is acknowledged. Because applicant did not distinctly and specifically point out the supposed errors in the restriction requirement, the election has been treated as an election without traverse (MPEP § 818.03(a)).

Claims 51 and 52 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected invention, there being no allowable generic or linking claim.

This application contains claims 51 and 52 drawn to an invention nonelected without traverse in the reply filed on 11/21/08. A complete reply to the final rejection must include cancellation of nonelected claims or other appropriate action (37 CFR 1.144) See MPEP § 821.01.

Specification

The amendment filed 7/25/06 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows:

Applicant adds the following new matter to page 6: *Regardless of whether a wired, or wireless connection is used, those aspects of the connection residing within the mobile phone 30 constitute means for connection to the PC 10 (which is external, and therefore remote from, the mobile phone 30) without involving the wireless communications network that the mobile phone 30 is additionally capable of communicating with.*

Applicant adds the following new matter to pages 10 and 11:

Regardless of whether a wired, or wireless connection is used, those aspects of the connection residing within the mobile phone 30 constitute means for connection to the PC 60 (which is external, and therefore remote from, the mobile phone 30) without involving the wireless communications network that the mobile phone 30 is additionally capable of communicating with.

Applicant is required to cancel the new matter in the reply to this Office Action.

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

The specification does not provide antecedent basis for the added limitation "*means for connection to a remote computer without involving the wireless communications network*", claimed within the amended claim 7.

Claim Objections

Claim 36 objected to because of the following informalities:

Applicant argues (e.g. see Remarks, pg. 16) that claim 36 should be interpreted as a system comprising a mobile communications device as opposed to a computer comprising a mobile communications device. The examiner respectfully notes then that the applicant's claim is improperly recited. Claim 36 should correctly recite:

A system for supporting an application, the system comprising*:*

a computer including a cryptographic application program interface and a cryptography service provider*;*

a mobile communication device including a cryptographic module*;*

wherein…

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 7 – 18 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. See objection to specification.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 47 and 48 are rejected under 35 U.S.C. 102(b) as being anticipated by Caputo et al., "Pocket Encrypting and Authenticating Communications Device", U.S. Patent 5,778,071.

Regarding claim 47, Caputo et al. discloses:

an application interface for connection to a computer application (2:47-55; 15:25-34)*; and an external interface for connection to a mobile communication device containing a cryptographic module wherein* (2:47-55)*, when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom* (Caputo et al., 15:13-39, 17:12-67; 18:1-9; figs. 3, 4a, 5a). Caputo discloses that the module commands the cryptographic module to encrypt data.

Regarding claim 48, Caputo et al. discloses:

wherein the module has some cryptographic functionality, and comprises means for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function (Caputo et al., Col. 15, lines 13-39). Caputo discloses a system comprising a module interfaced with a cryptographic module for purposes of providing cryptographic functionality. Computerized modules operate in response to commands and requests, such as sets of instructions, codes, or signals. Consequently, the module comprises means to provide the requested cryptographic function (establish that it is capable of providing the requested cryptographic function).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 4, 6, 7, 11, 13 – 15, 18, 19, 24, 26 – 28, 32 – 34, 36 – 39, 42, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo et al. (Caputo), "Pocket Encrypting and Authenticating Communications Device", U.S. Patent 5,778,071 in view of Liebenow et al. (Liebenow), "Dual Mode Modem for Automatically Selecting Between Wireless and Wire-based Communication Modes", U.S. Patent 6,131,136.

Regarding claim 1, Caputo et al. discloses a method of authenticating communications, the method comprising:

initiating communications from said computer over a computer network (Caputo, fig. 3 – Herein Caputo discloses a computer network comprising: a computer 36 connected to a security system 38 connected to a modem 30 connected to a network 20 connected to a token 10 connected to a computer 22)*; determining that encryption of said communications is required; establishing a connection with a mobile communications device* (i.e. token 10)*, wherein said mobile communications device*

includes a cryptographic module for use in mobile communication (Caputo, fig. 3; 9:46-60; 15:13-39).

Caputo discloses a mobile communications device with a modem (Caputo, fig. 3:10; fig. 2:160). The modem is shown to connect to a wired communications network (Caputo, fig. 3:14). Caputo does not disclose that the mobile communication device is also usable over a wireless communications network.

Liebenow discloses that mobile communication devices should possess modems with the ability to communicate via both wired and wireless communications networks (Liebenow, fig. 1:107, 105). Liebenow discloses that such an arrangement offers mobile communication devices the flexibility and convenience to communicate with whichever type of network is available and further protects the mobile communications device from the misuse of power (Liebenow, Abstract, 1:13-26; 1:65 – 2:5).

It would have been obvious to one of ordinary skill in the art to employ the dual modem features of Liebenow within the mobile communication device of Caputo. This would have been obvious because one of ordinary skill in the art would have been motivated by benefits of flexibility and power usage protection as taught by Liebenow.

Thus, the combination of Caputo and Liebenow disclose:

over a wireless communications network (Caputo, fig. 4a:40; Liebenow, fig. 1:107);

using the cryptographic module of the mobile communications device as an cryptographic service provider for encrypting said communications from said computer over said computer network (Caputo, fig. 3:36,38,30,20,10,22; 9:46-60; 15:13-39; 2:23-

27; 3:33-38) *without sending said encrypted communications over said wireless communications network* (Liebenow, fig. 1:105 and Caputo, fig. 3 vs. Liebenow, fig. 1:107).

Regarding claim 4, the combination of Caputo and Liebenow disclose:

wherein the step of establishing a connection with the mobile communications device comprises establishing a wired connection between the mobile communications device and the computer (Caputo; fig. 3).

Regarding claim 6, the combination of Caputo and Liebenow disclose:

when the application program interface requires cryptographic functionality, calling a cryptographic service provider function in the mobile communications device (Caputo, 15:13-39).

Regarding claim 7, it is rejected, at least, for the same reasons as claim 1, and furthermore because the combination of the combination of Caputo, Liebenow, and Geiger disclose:

means for communicating over a wireless interface with a wireless communications network (Caputo, fig. 4a:40; Liebenow, fig. 1);

means for connection to a remote computer without involving the wireless communications network (Caputo, fig. 3);

and a cryptographic module, the cryptographic module being usable: for encoding wireless communications from the device over said wireless interface; by a cryptographic service provider with an application program interface of the remote computer (Caputo et al., Col. 2, lines 23-27; Col. 3, lines 33-38, 46-50; Col. 15, lines 13-39, figs. 2, 3, 4a, 5a; Liebenow, fig. 1).

Regarding claim 11, the combination of the combination of Caputo and Liebenow disclose:

wherein the cryptographic module uses public key cryptography (Caputo et al., Col. 1, lines 27-39; Col. 11, lines 18-59).

Regarding claim 18, the combination of the combination of Caputo and Liebenow disclose:

an interface for receiving a command from a personal computer, the mobile communications device acting as a cryptographic service provider for said personal computer in response to said command (Caputo et al., Col. 15, lines 13-39).

Regarding claim 19, it is rejected, at least, for the same reasons as claim 1, and furthermore because the combination of Caputo et al. and Liebenow disclose:

a tangible module for a personal computer, wherein, in response to the module receiving a first command from a cryptographic application program interface, indicating that it requires cryptographic functionality for communication over a computer network,

the module sends a second command to a mobile communication device, the mobile communication device having a cryptographic module for use in mobile communication over a wireless communications network, such that the cryptographic module acts as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network (Liebenow, fig. 1; Caputo, fig. 3; 15:13-39; 17:12-67; 18:1-9). The combination of Caputo and Liebenow disclose a system comprising an application program running on a computer, the application being interfaced with a cryptographic module for purposes of providing cryptographic functionality. Computer applications, as well as the cryptographic module, operate using commands, such as sets of instructions, codes, or signals. When the application is instructed to utilize the cryptographic module, commands are sent to enable such usage.

Regarding claim 24, it is rejected, at least, for the same reasons as claim 1, and furthermore because the combination of Caputo and Liebenow disclose:

a computer; and mobile communications device, including a cryptographic module for performing cryptographic functions in mobile communication over a wireless communications network, the computer having at least one application which requires cryptographic functionality for communication over a computer network, a first part of the required cryptographic functionality being provided in the computer, and a second part of the required cryptographic functionality being provided in the mobile

communications device (Liebenow, fig. 1; Caputo 15:13-39, col. 9, lines 28-36). As disclosed, each of the computer and the mobile communications device cooperate to provide the resulting cryptographic functionality. Thus, the computer and the mobile device provide first and second parts of cryptographic functionality. Additionally, the computer provides instructions for the operation of the encrypting device, including functionality for the manipulation of encryption modes, and combining unencrypted data with encrypted data to submission to further encryption processing. The device executes an encryption algorithm for encrypting the data submitted by the computer.

the computer and the mobile communications device having means for establishing a secure communications path there between (Caputo et al., fig. 3); *and the computer further comprising an interface device which, on determining that an application needs use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends command thereto* (Caputo et al., Col. 15, lines 13-39).

Regarding claim 26, Caputo et al. discloses:

wherein the computer application which requires cryptographic functionality is an internal memory access application (Caputo et al., Col. 15, lines 13-39).

Regarding claim 27, Caputo et al. discloses:

wherein the computer application which requires cryptographic functionality is an external communication application (Caputo et al., Col. 15, lines 13-39).

Regarding claims 28, it is rejected, at least, for the same reasons as claim 1, and furthermore because the combination of Caputo and Liebenow disclose:

sending data to be encrypted from the computer to a mobile communications device, wherein the mobile communications device has a cryptographic module for performing cryptographic functions in communications over a wireless communications network, and further, wherein the mobile communications device uses the cryptographic module to encrypt the data (Caputo, fig. 3; 9:46-60; 15:13-39; 2:23-27; 3:33-38);

receiving the encrypted data at the computer from the mobile communications device (Caputo, 15:13-39);

and using the encrypted data in communications over the computer network without sending the encrypted data over the wireless communications network (Caputo, fig. 3; 15:13-39).

Regarding claims 32 and 33, the combination of Caputo and Liebenow discloses:

using a cryptographic module realized in hardware in the mobile communications device and *using a cryptographic module realized in software in the mobile communications device* (Caputo et al., Col. 9, lines 40-45).

Regarding claims 34, the combination of Caputo and Liebenow discloses:

using a cryptographic module provided on an external smart card which can be read by the mobile communications device (Caputo et. al., Col. 10, lines 19-31, 51-59; Col. 13, lines 4-10, 25-67).

Regarding claims 13, 14, and 15, they are substantially similar to claims 32, 33, and 34 and they are rejected, at least, for the same reasons.

Regarding claim 36, it is rejected, at least for the same reasons as claim 1, and furthermore because the combination Caputo and Liebenow disclose:

a computer including: a cryptographic application program interface; and a cryptography service provider; and a mobile communication device including a cryptographic module, wherein, when the cryptographic application program interface determines that the application requires cryptographic functionality for communication over a computer network, the cryptographic application program interface, sends a command to the cryptography service provider (Caputo et al., Col. 15, lines 13-39), *and wherein the cryptography service provider has a communications link to the cryptographic module of the mobile communications device, the cryptographic module of the mobile communications device being usable to encrypt communications between the mobile communications device and a telecommunications network over a wireless interface* (Caputo et al., fig. 3: Liebenow, fig. 1), *and wherein the cryptography service provider can obtain the cryptographic functionality, required by the application, from the cryptographic module of the mobile communications device* (Caputo et al., Col. 2, lines

23-27; Col. 3, lines 33-38) *without the mobile communications device sending the encrypted communications over the telecommunications network* (Caputo, 15:13-39).

Regarding claims 37, 38, 39, they are substantially similar to claims 32, 33, and 34 and they are rejected, at least, for the same reasons.

Regarding claim 42, the combination of Caputo and Liebenow discloses:

wherein the cryptography service provider has some cryptographic functionality (Caputo, 15:13-39),

and, on receipt of a command form the cryptographic application program interface, determines whether it can perform the required cryptographic functionality, or whether to obtain the required cryptographic functionality from the cryptographic module of the mobile communications device (Caputo 15:13-39). Caputo discloses a system comprising a module interfaced with a cryptographic module for purposes of providing cryptographic functionality. Computerized modules operate in response to commands and requests, such as sets of instructions, codes, or signals. Consequently, the module comprises means to provide the requested cryptographic function (establish that it is capable of providing the requested cryptographic function).

Regarding claim 44, it is rejected, at least, for the same reasons as claim 1, and furthermore because the combination of Caputo and Liebenow disclose:

the mobile communications device being able to communicate over a first wireless interface with a telecommunications network, and comprising a cryptographic module to provide cryptographic functionality for use in communications over the first wireless interface (Caputo, fig. 3; Liebenow, fig. 1), *the mobile communications device further comprising a security manager module for receiving commands from a computer system over a second interface* (Caputo, fig. 2)*, wherein, in response to suitable commands received from the computer system over the second interface, the security manager module requests a cryptographic function from the cryptographic module, and returns the results of the cryptographic function to the computer system over the second interface, without sending the results of the cryptographic function over the first wireless interface* (Caputo et al., Col. 15, lines 13-39).

Claims 5, 8, 9, 41, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Caputo and Liebenow in view of Ericsson, "Bluetooth – A Global Specification for Wireless Connectivity".

Regarding claims 5, 8, 9, 41, and 46, the combination of Caputo and Liebenow disclose a wired connection between the device and the computer (Caputo et al., Col. 6, lines 41-61). The combination does not disclose a wireless connection or connection via a short-range transceiver incorporating Bluetooth wireless technology.

Ericsson discloses the obvious use of wireless connections between devices (Ericsson, Page 1). Bluetooth, a short-range radio technology allows for the

replacement of wired connections – "facilitating protected" wireless connections between mobile devices. As disclosed, Bluetooth technology can be used to replace "the cumbersome cable used today to connect a laptop to a cellular telephone".

It would be obvious to one of ordinary skill in the art to employ the secure feature of wireless short-range radio connection and Bluetooth technology of Ericsson with the combination of Caputo and Liebenow because it is apparent that the ability to securely operate wirelessly would enhance a security/communication device designed to be mobile and portable.

Claim 49 is rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo in view of Ericsson, "Bluetooth – A Global Specification for Wireless Connectivity".

Regarding claim 49, Caputo discloses a wired connection between the device and the computer (Caputo et al., Col. 6, lines 41-61). Caputo does not disclose a wireless connection or connection via a short-range transceiver incorporating Bluetooth wireless technology.

Ericsson discloses the obvious use of wireless connections between devices (Ericsson, Page 1). Bluetooth, a short-range radio technology allows for the replacement of wired connections – "facilitating protected" wireless connections between mobile devices. As disclosed, Bluetooth technology can be used to replace "the cumbersome cable used today to connect a laptop to a cellular telephone".

It would be obvious to one of ordinary skill in the art to employ the secure feature of wireless short-range radio connection and Bluetooth technology of Ericsson within the system of Caputo because it is apparent that the ability to securely operate wirelessly would enhance a security/communication device designed to be mobile and portable.

Claims 2, 3, 10, 12, 16, 17, 25, 29, 30, 35, and 40, are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Caputo and Liebenow in view of Geiger et al. (Geiger), "Secure Wireless Electronic-Commerce System with Wireless Network Domain", U.S. Patent 6,463,534 B1.

The combination of Caputo and Liebenow disclose a mobile communications device, comprising a cryptographic module, which is used as a token for authenticating a user and for encrypting communications (Caputo, 2:23-27; 3:33-38, 46-50; Fig. 2). The device sends communications to a recipient by wired telephonic means or wireless telephonic means (Caputo, Fig. 2:14; 16:40-45; 17:3-7; Liebenow, fig. 1). The combination of Caputo and Liebenow, however, does not disclose that the wireless mobile communications device is enabled to use the enhanced wireless security of the Wireless Application Protocol.

Geiger et al., discloses a wireless mobile device and system used to send secure wireless communication using the Wireless Application Protocol (Geiger, 2:49-65; 9:22-

53; 11:64 – 12:8). As disclosed by Geiger et al., WAP (utilizing WTLS and a WIM) is a convenient protocol to use with wireless mobile communications, chosen for its security.

Thus, it would have been obvious to one of ordinary skill in the art to employ the secure Wireless Application Protocol feature of Geiger et al. with the combination of Caputo and Liebenow because it is obvious that a wireless mobile communication device designed for authenticated and encrypted communications would be enhanced by the use of a convenient communication protocol and system that features increased wireless security.

Regarding claim 2, the combination of Caputo, Liebenow, and Geiger disclose: *the mobile communications device is a WAP-enabled device* (Geiger et al., Fig. 1, Col. 9, lines 22-53). As disclosed, the device is WAP-enabled since it communicates using the WAP protocol.

Regarding claim 3, the combination of Caputo, Liebenow, and Geiger disclose: *wherein the cryptographic module is that used by the mobile communications device for Wireless Transport Layer Security communications* (Geiger et al., Col. 2, lines 49-65; Col. 6, lines 55-58; Col. 9, lines 22-53). As disclosed, communication security, the functionality provided by the cryptographic module, is accomplished using WTLS communications.

Regarding claim 10, it is substantially similar to claim 3, and is rejected for the same reasons.

Regarding claim 12, the combination of the combination of Caputo, Liebenow, and Geiger disclose:

means for sending and transmitting data using WAP (Geiger et al., Fig. 1, Col. 9, lines 22-53).

Regarding claims 16 and 17, the combination of the combination of Caputo, Liebenow, and Geiger disclose:

wherein the cryptographic module comprises a Wireless Identity Module card and *wherein the cryptographic module comprises a Wireless Identity Module card which allows communications using Wireless Transport Layer Security.* (Geiger et al., col. 11, line 64 – col. 12, line 8; fig. 4, elems. 450, 452).

Regarding claims 25, 29, and 30, they are substantially similar to claims 2 and 3, and they are rejected for the same reasons.

Regarding claims 35 and 40, they are substantially similar to claims 16, and are rejected, at least, for the same reasons.

Claims 43 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Caputo and Liebenow in view of RSA, "PKCS #11 v2.10: Cryptographic Token Interface Standard".

Regarding claims 43 and 45, the combination of Caputo and Liebenow discloses a portable encryption and authentication device. The device utilizes a modem and "industry compatible" modem commands for communication (Caputo, 2:160; 17:12-35; 16:40-61). The combination, however, does not disclose specifically that the mobile communications device utilizes PKCS #11 with AT commands.

RSA discloses that the PKCS #11 command set is the industry standard for encryption and authentication devices (RSA, pages 1-12).

It would have been obvious to one of ordinary skill in the art to employ PKCS #11 command set, disclosed by RSA to be the industry standard, in the combination of Caputo, Liebenow, and Geiger. This would have been obvious because one of ordinary skill in the art would have been motivated for the purpose of utility and compatibility to utilize the standards defined by industry. Furthermore, the disclosure of AT commands is obvious as these are the standard industry commands used to communicate via modems, as evidenced by the definitions of "AT Command Set" and "Modem Standards" in Newton's Telecom Dictionary, 13th ed.

Claim 50 is rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo in view of RSA, "PKCS #11 v2.10: Cryptographic Token Interface Standard".

Regarding claim 50, Caputo discloses a portable encryption and authentication device. The device utilizes a modem and "industry compatible" modem commands for communication (Caputo, 2:160; 17:12-35; 16:40-61). Caputo, however, does not disclose specifically that the mobile communications device utilizes PKCS #11 with AT commands.

RSA discloses that the PKCS #11 command set is the industry standard for encryption and authentication devices (RSA, pages 1-12).

It would have been obvious to one of ordinary skill in the art to employ PKCS #11 command set, disclosed by RSA to be the industry standard, in the system of Caputo. This would have been obvious because one of ordinary skill in the art would have been motivated for the purpose of utility and compatibility to utilize the standards defined by industry. Furthermore, the disclosure of AT commands is obvious as these are the standard industry commands used to communicate via modems, as evidenced by the definitions of "AT Command Set" and "Modem Standards" in Newton's Telecom Dictionary, 13th ed.

Response to Arguments

Applicant's arguments filed 11/21/08 have been fully considered but they are not persuasive.

Applicants argues essentially that:

(i) *As for the "means for connection to a remote computer without involving the wireless communications network", this is depicted in each of Figures 1 and 4 …* (Remarks, pg. 13)

Claim 7 was similarly amended to define "means for connection to a remote computer without involving the wireless communications network." (Remarks, pg. 17)

In response, the examiner respectfully notes that the applicant fails to disclose the concept of ***"without involving"*** a wireless network. Nowhere within the applicant's original disclosure does the applicant define "involvement" and "without involvement". The examiner respectfully notes that the applicant's arguments appear to successfully point out the support for claim language such as "without sending" over a wireless network. The examiner respectfully suggests that similar recitations within claims 7 - 18 would appear to address the issues raised by the rejection.

(ii) *While Applicant strongly disagrees that the proposed amendments filed on July 25, 2006 introduced new subject matter into the disclosure, the issue was long ago rendered moot by the Office' s Advisory Action of August 4, 2006, in which Box 3 has*

been checked to indicate "The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because ... (b) They raise the issue of new matter (see NOTE below); (c) They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal .... "

That is, the Office is now objecting to language that is not part of the specification. This being the case, there is nothing that Applicant can do to address the Office's concern. It is therefore respectfully requested that this objection to the specification be withdrawn. (Remarks, pg. 15)

In response, the examiner respectfully notes that the applicant appears to be mistaken. Specifically, the applicant's amendment after final of 7/25/06 was entered by virtue of the Office's re-opening of the prosecution after appeal by applicant. Please refer to M.P.E.P 1207.04 [R-3]:

"Reopening of Prosecution After Appeal… Any after final amendment or affidavit or other evidence that was not entered before must be entered and considered on the merits."

Therefore, the examiner respectfully notes that the applicant's remarks must address the issues raised by the Non-Final office action of 10/9/07.

(iii) *Neither of claims 47 and 48 is anticipated by Caputo because Caputo fails to disclose or suggest a division of cryptographic functions wherein some are performed within the computer itself and others are performed within a cryptographic module*

located in a mobile communications device so that the computer comprises "a cryptographic module; wherein, ***when the module receives from the application interface a request for a cryptographic function which the module is unable to provide****, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom," as defined by claim 47. Caputo is similarly silent with respect to claim 48's recitation of "****the module [having] some cryptographic functionality****, and compris[ing] means for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function." (Emphasis added.)*

… Nowhere does this passage describe a computer having its own cryptographic capabilities separate and apart from those provided by the device 10. (Remarks, pg. 20, 21)

D. Neither Caputo nor Liebenow disclose a system in which "a first part of the required cryptographic functionality .ty [is] provided in the computer, and a second part of the required cryptographic functionality [is] provided in the mobile communications device" (Remarks, pg. 26)

As Caputo is lacking any disclosure of some cryptographic functionality being performed in the computer, and some cryptographic functionality being performed in the mobile communications device, it follows that Caputo does not describe an interface for selecting one of the two. Liebenow, which is silent with respect to cryptographic functionality, fails to make up for the deficiencies of Caputo. (Remarks, pg. 26, 27)

In response, the examiner points out that the prior art shows separate elements in cooperation for the provision of cryptographic functionality. Thus the elements provide cryptographic functionality (See above rejections). For example the mobile device can transform data via an encryption algorithm (i.e. a cryptographic functionality provided by the device) whereas the computer can construct encrypted messages (i.e. a cryptographic functionality" provided by the computer) (Caputo, 15:15-40). It is clearly seen that the each element provides a cryptographic functionality, wherein the computer does not transform data via an encryption function as does the mobile device and the mobile device does not construct encrypted messages as does the computer.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *its own cryptographic capabilities separate and apart from those provided by the device*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Furthermore, in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

(iv) *…the cryptographic circuitry disclosed by Caputo is not "for use in mobile communication over a wireless communications network" as variously required by the claims…* (Remarks, pg. 23)

In response, the examiner respectfully notes that rejections made in view of the combination of Caputo and Liebenow clearly addresses cryptographic circuitry for communications over a wireless network (Caputo fig. 2:160; Liebenow, fig. 1:109, 111).

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

(v) *Neither Caputo nor Liebenow disclose "using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network"* (Remarks, pg.24)

In response, the examiner respectfully notes that the combination clearly shows *"using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer*

over said computer network" (Caputo, fig. 3; Liebenow, fig. 1:105) *"without sending said encrypted communications over said wireless communications network"* (Liebenow, fig. 1:105 vs. 107).

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

(vi) *Neither Caputo nor Liebenow disclose a dual-mode cryptographic module that is both "for use …* (Remarks, pg. 25)

In response, the examiner respectfully notes that the prior art combination clearly enables "a dual mode" device for the intended use recitation as claimed by the applicant (Caputo, fig. 2:160; Liebenow, fig. 1).

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

(vii) *Any combination of Caputo's teachings with the teachings of Liebenow would still lack features variously defined by Applicant's claims.*

The Office Action acknowledges that Caputo does not disclose, at least, a mobile communication device that is also usable over a wireless communications network, but relies on Liebenow as making up for this deficiency. This reliance is unfounded, at least for the reasons discussed above in Sections A through E. (Remarks, pg. 27)

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

The examiner respectfully notes that this argument is premised upon the arguments found to be unpersuasive above, and it is unpersuasive for the same reasons.

(viii) *Moreover, Applicant believes that Liebenow cannot be considered to disclose a mobile communication device, as that term is used in Applicant's specification.* (Remarks, pg. 27)

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections

are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Furthermore, the examiner respectfully notes for the applicant's benefit that the device disclosed by Liebenow clearly would enable a "mobile" device, since the device of Liebenow is a portable device for cellular phone communications (Liebenow, 1:11-25; 2:51-60).

(ix) *Moreover, even if Caputo' s device were modified to include Liebenow' s dual mode capability, the combination would still operate in only one mode, namely, for the benefit of the external device (computer), operating only to pass data between the computer and its network. All cryptographic functions would be performed only as required by the node that the computer is connected to, and would pass through the device to the computer network. By contrast, embodiments such as those defined by independent claim 28 require that the encrypting device return the encrypted data to the computer for communication over a computer network without sending the encrypted data over the wireless communication network.* (Remarks, pg. 27)

In response, the examiner respectfully notes that the applicant fails to provide any rational or evidence for the assertion that the "dual mode" device as enabled by the prior art combination would only operate in one mode.

Furthermore, the examiner points out that the claim recitations themselves only show operating in "one mode" (i.e. *for communication over a computer network without sending the encrypted data over the wireless communication network*).

Conclusion

The following prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See Notice of References Cited.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFERY WILLIAMS whose telephone number is (571)272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

J.Williams
AU: 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437